S9L5 – RELAZIONE PROGETTO SETTIMANALE

Traccia

Con riferimento alla figura in basso, rispondere ai seguenti quesiti.

1. **Azioni preventive**: quali azioni preventive si potrebbero implementare per difendere l'applicazione Web da attacchi di tipo SQLi oppure XSS da parte di un utente malintenzionato? Modificate la figura in modo da evidenziare le implementazioni. È richiesta sola modifica
2. **Impatti sul business**: l'applicazione Web subisce un attacco di tipo l'applicazione non raggiungibile per 10 minuti. DDoS dall'esterno che rende Calcolare l'impatto sul business dovuto alla non raggiungibilità del servizio, considerando che in media minuto gli utenti spendono ogni 1.200 € sulla piattaforma di e-commerce. Fare eventuali valutazioni di azioni preventive che si possono applicare in questa problematica
3. **Response**: l'applicazione Web viene infettata da un malware. La vostra priorità è che il malware non si propaghi sulla vostra rete, mentre non siete interessati a rimuovere l'accesso da parte dell'attaccante alla macchina infettata.
   Modificate la figura in slide 2 con la soluzione proposta.
4. **Soluzione completa**: unire i disegni dell'azione preventiva e della response (unire soluzione 1 e 3)
5. **Modifica «più aggressiva» dell'infrastruttura**: integrando eventuali altri elementi di sicurezza (**integrando anche una soluzione al punto 2**) Budget 5000-10000 euro. Eventualmente fare più proposte di spesa.

Svolgimento

Azioni Preventive

Per prevenire uno scenario di compromissione di un'applicazione web come un sito e-commerce aziendale da attacchi **XSS** e **SQLi** è necessario inserire un firewall aggiuntivo a protezione della **DMZ**.

La scelta del tipo di firewall dipende dal campo di applicazione dello stesso, in questo caso abbiamo una Web Application E- Commerce e di conseguenza la nostra miglior scelta sarà un firewall di tipo **Web Application Firewall WAF**.

Proteggere un'applicazione di e-commerce è essenziale per garantire la sicurezza dei dati degli utenti e delle transazioni. Un Web Application Firewall (WAF) è spesso la scelta migliore per diversi motivi.

Protezione Mirata per Applicazioni Web

I WAF sono pensati specificamente per le applicazioni web e sono ottimizzati per riconoscere e bloccare attacchi come SQL Injection (SQLi) e Cross-Site Scripting (XSS).

Questo li rende particolarmente efficaci per le piattaforme di e-commerce, dove proteggere le informazioni degli utenti è fondamentale.

Riduzione dei Rischi Specifici

Le piattaforme di e-commerce sono un bersaglio comune per gli hacker che cercano di rubare informazioni sensibili, come i dati di pagamento.

I WAF possono essere configurati per proteggere aree critiche come i moduli di pagamento e login, offrendo un ulteriore livello di protezione.

Filtraggio e Monitoraggio del Traffico

Un WAF non solo filtra il traffico in entrata, ma può anche bloccare richieste sospette e fornire report dettagliati sulle minacce.

Questo permette di individuare e affrontare le vulnerabilità prima che vengano sfruttate.

Facilità di Implementazione

I WAF sono spesso disponibili come servizi cloud o appliance hardware, che possono essere facilmente integrati e configurati senza richiedere grandi modifiche all'infrastruttura esistente.

Conformità alle Normative

Per le piattaforme che gestiscono informazioni di pagamento, è essenziale rispettare standard di sicurezza come il PCI DSS.

Un WAF può aiutare a soddisfare questi requisiti implementando le necessarie misure di protezione.

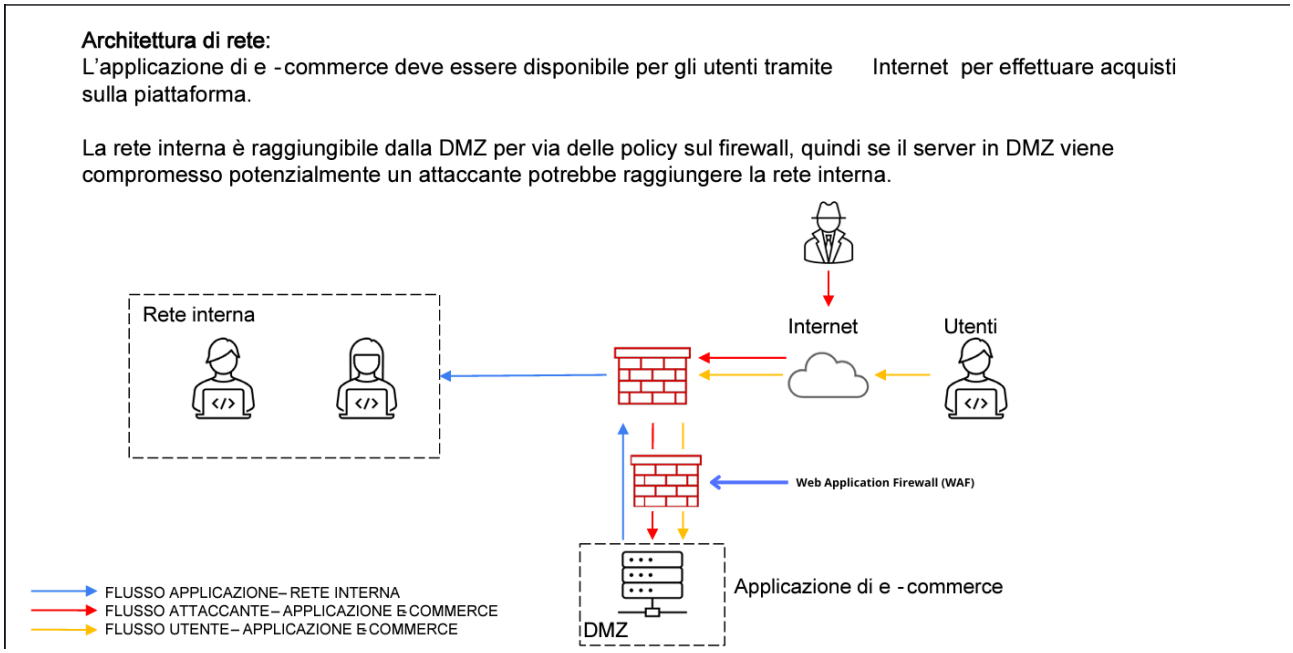
Considerazioni sull'Uso di un WAF

Nonostante l'efficacia di un WAF, è importante ricordare che non sostituisce altre misure di sicurezza.

È fondamentale adottare un approccio di difesa stratificata, che includa aggiornamenti regolari del software, pratiche di sviluppo sicure e un monitoraggio costante per individuare e rispondere prontamente alle minacce.

In sintesi, un WAF è uno strumento essenziale per proteggere le piattaforme di e-commerce, ma deve essere parte di una strategia di sicurezza più ampia per garantire una protezione completa.

Architettura di rete con aggiunta del WAF



Impatti sul business

Per calcolare l'impatto economico dell'attacco DDoS che rende l'applicazione non raggiungibile per 10 minuti, possiamo utilizzare la spesa media degli utenti come dato principale.

Calcolo dell'impatto economico

- **Spesa media per minuto:** 1.200 €
- **Durata del downtime:** 10 minuti

L'impatto economico si calcola moltiplicando la spesa media per minuto per il numero di minuti in cui l'applicazione non è stata raggiungibile:

Impatto economico=1.200 €×10 min=12.000 €

Impatto economico totale: 12.000 €

Azioni Preventive per Mitigare i DDoS

Per evitare o ridurre l'impatto di attacchi DDoS in futuro, alcune azioni preventive che si possono considerare includono:

1. **Distribuzione e Bilanciamento del Carico:**
    - Utilizzare soluzioni di bilanciamento del carico per distribuire il traffico tra più server, riducendo il rischio che un singolo server venga sovraccaricato.
2. **Mitigazione DDoS:**
    - Implementare soluzioni specializzate per la mitigazione DDoS che possono identificare e filtrare il traffico malevolo, mantenendo il servizio operativo.
3. **Ridondanza dell'Infrastruttura:**
    - Creare infrastrutture ridondanti con capacità di failover per garantire la disponibilità del servizio anche in caso di attacco.
4. **Aumento della Larghezza di Banda:**
    - Aumentare la larghezza di banda disponibile può aiutare a gestire l'aumento improvviso del traffico dovuto a un attacco DDoS.
5. **Monitoraggio e Allerta:**
    - Implementare strumenti di monitoraggio per rilevare rapidamente comportamenti anomali nel traffico e avvisare il team di sicurezza per una risposta tempestiva.

Response

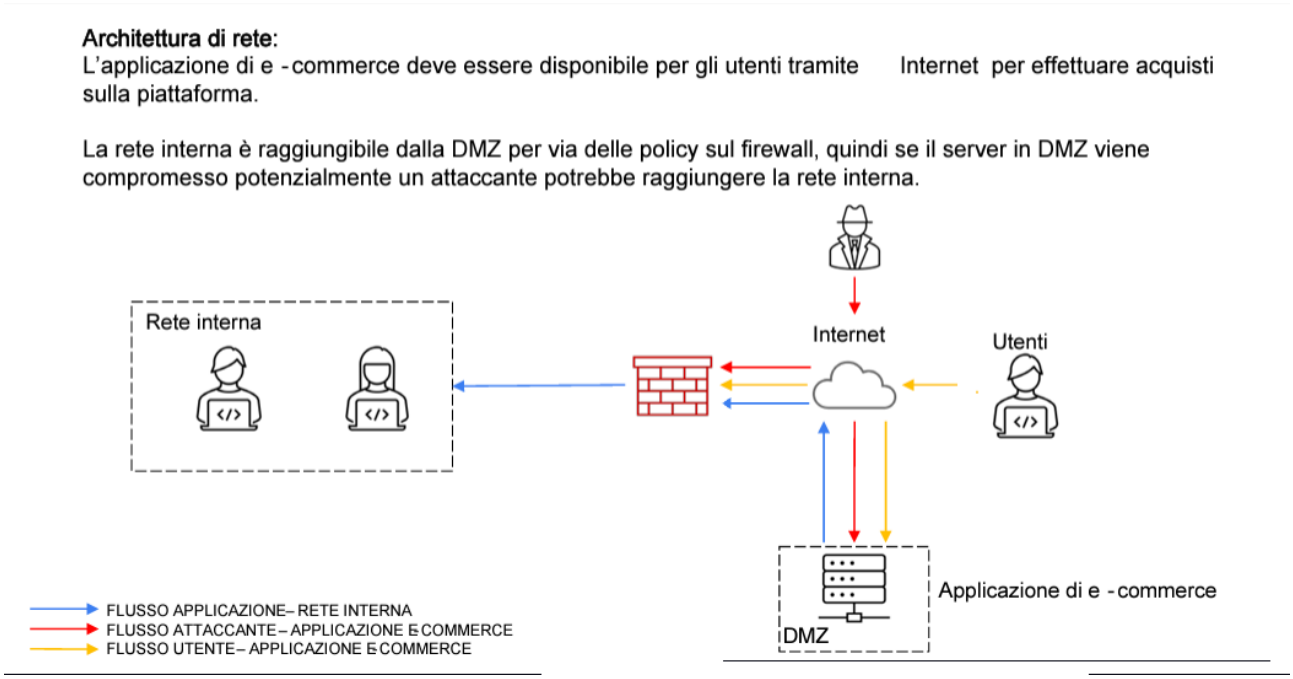
Nel caso in cui la nostra applicazione web venisse infettata da dei malware potremmo andare ad agire sulla rete in modo da poter isolare la nostra DMZ.

Tenendo a mente ciò, creiamo una VLAN distinta dalla nostra rete interna e la aggiungiamo alla tabella di routing del firewall.

In questo modo la rete appena creata potrà comunicare con la rete interna ma allo stesso tempo quest’ultima sarà al sicuro rete dai malware presenti nella nostra DMZ

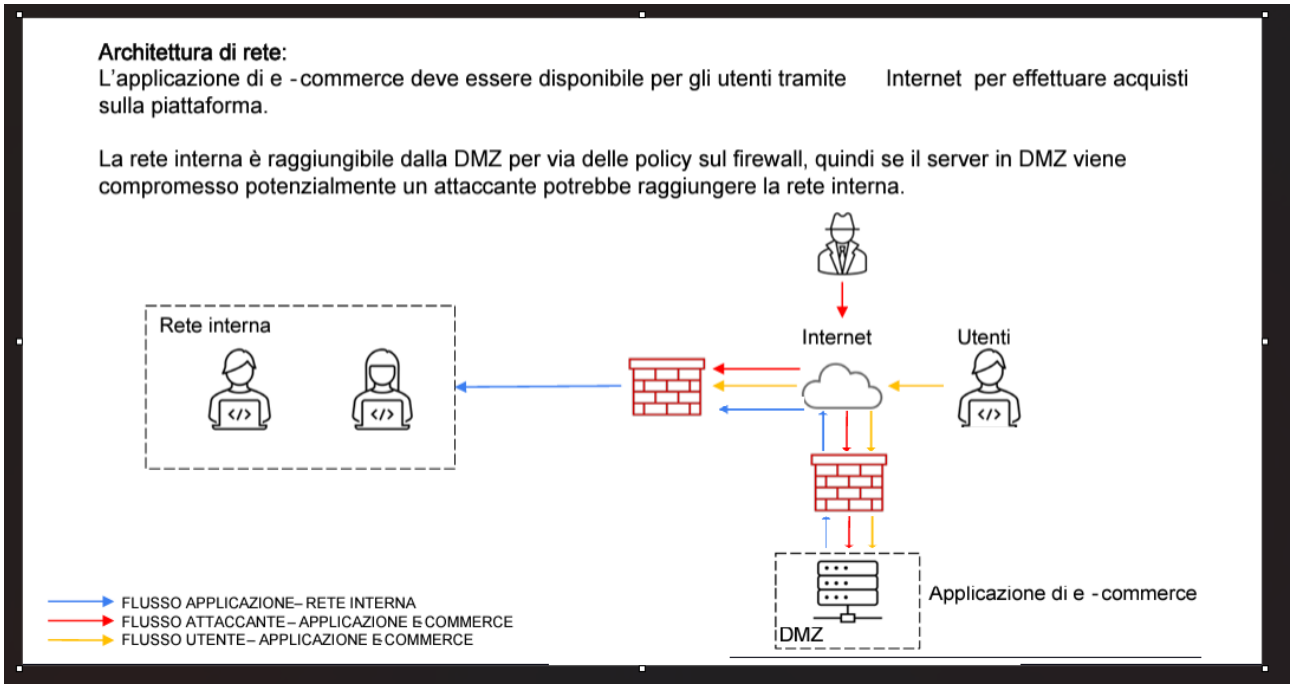
A questo punto possiamo collegare la DMZ ad internet

Potete trovare uno schema di ciò di seguito:



Soluzione completa

Di seguito trovate le soluzioni 1 e 3 unite in un'unica soluzione:



In questo schema possiamo vedere come prevenire un possibile attacco SQLi o XSS dividendo le reti in due:

- Rete Interna
- Rete DMZ

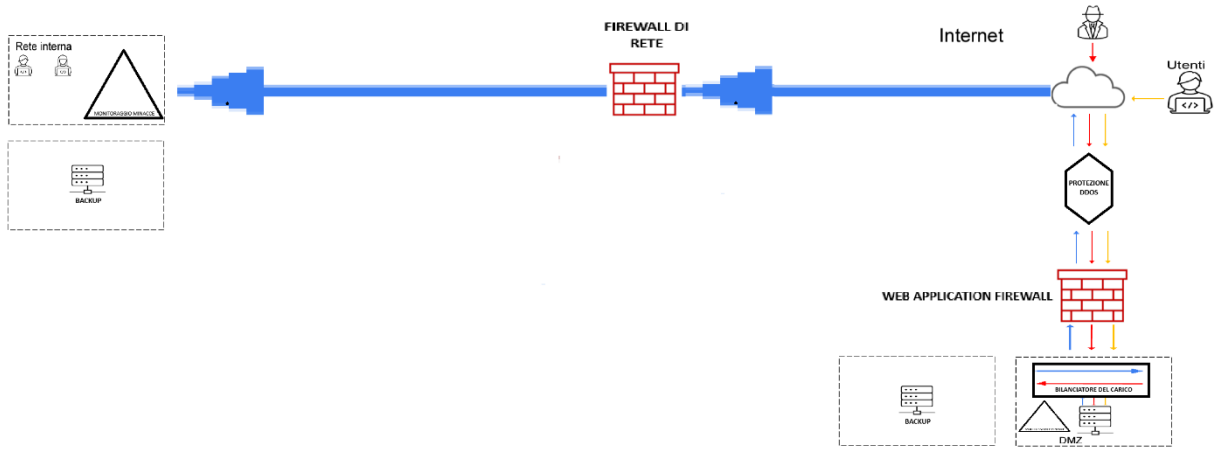
Successivamente andiamo a posizionare un firewall di rete tra la nostra rete interna ed internet, nelle impostazioni di questo firewall andiamo a configurare la tabella di routing la quale dovrà essere popolata da una regola che consenta il passaggio di tutti gli indirizzi di rete della nostra rete interna e dovrà rifiutare qualsiasi altro indirizzo.

In questo modo la nostra rete interna sarà protetta dall'esterno.

Per quanto riguarda la DMZ invece procederemo con l'inserimento di un Web Application Firewall, il quale come abbiamo detto prima, è pensato specificamente per le applicazioni web e sono ottimizzati per riconoscere e bloccare attacchi come SQL Injection (SQLi) e Cross-Site Scripting (XSS).

In questo modo un potenziale attaccante potrà comunque avere accesso alla WA ma in caso di tentativo di attacco il WAF riconoscerà la tipologia di attacco e prenderà le giuste contromisure per prevenirlo.

Modifica «più aggressiva» dell'infrastruttura integrando anche una soluzione al punto 2



Ecco un elenco dettagliato delle soluzioni per migliorare la sicurezza della rete e dell'applicazione di e-commerce, con un budget massimo di €10,000:

1. **Web Application Firewall (WAF)**
    - **Costo stimato**: € 3000
    - **Descrizione**: Un WAF protegge le applicazioni web da attacchi come SQL injection e cross-site scripting. Questo può essere implementato come

appliance hardware (ad es., Fortinet, Barracuda) o come servizio cloud (ad es., AWS WAF, Cloudflare).

2. **Protezione DDoS**
    - **Costo stimato**: € 2000
    - **Descrizione**: La protezione DDoS aiuta a mitigare attacchi che mirano a sovraccaricare il sistema con traffico malevolo. Servizi come Cloudflare, Akamai o Imperva offrono soluzioni che filtrano e bloccano il traffico sospetto.
3. **Bilanciamento del Carico**
    - **Costo stimato**: € 1500
    - **Descrizione**: Un bilanciatore di carico distribuisce il traffico tra vari server, migliorando la disponibilità e prevenendo sovraccarichi. Soluzioni hardware (ad es., F5 Networks, Citrix) o servizi cloud (ad es., AWS Elastic Load Balancing) sono opzioni comuni.
4. **Infrastruttura Ridondante**
    - **Costo stimato**: Variabile, ma spesso intorno a € 1500 per componenti base
    - **Descrizione**: La ridondanza dell'infrastruttura assicura che ci siano backup server e sistemi di failover per mantenere il servizio operativo in caso di guasti. Questo può includere la duplicazione di server o l'utilizzo di servizi di cloud computing per backup.
5. **Aumento della Larghezza di Banda**
    - **Costo stimato**: €700
    - **Descrizione**: Incrementare la larghezza di banda disponibile aiuta a gestire picchi di traffico, specialmente durante un attacco DDoS. Questo può essere negoziato con il provider di servizi internet.
6. **Monitoraggio e Allerta**
    - **Costo stimato**: € 800
    - **Descrizione**: Strumenti di monitoraggio come SolarWinds, Nagios o servizi cloud (ad es., AWS CloudWatch) permettono di rilevare e segnalare attività anomale, facilitando una risposta tempestiva a potenziali minacce.

Totale Stimato:

Il totale stimato per queste soluzioni è di €9 500.